

Índice

1.	Sistemas de resolución de nombres	2
1.1	NetBIOS	2
1.2	WINS	3
2.	DNS.....	4
2.1	Funciones de DNS.....	4
2.2	Terminología.....	4
2.3	Estructura Jerárquica de Nombres.....	5
2.4	Relación entre zonas y servidores DNS.....	6
2.5	Proceso de resolución de nombres por un servidor DNS.....	8
2.6	Clientes DNS	8
2.7	Servidores DNS	10
2.8	Ficheros de zona	10
2.9	Resolución inversa	14
2.10	Utilizar DNS para asegurar los remitentes de correo	14
	Tipos de registro SPF	15
2.11	DNSSEC.....	15

1. Sistemas de resolución de nombres

Normalmente, los usuarios conocen el nombre de un host, pero no su dirección IP. Sin embargo, el ordenador necesita conocer la dirección para poder comunicarse con él. Por tanto, debe existir un mecanismo para obtener la dirección a partir del nombre de un host determinado.

Las redes pequeñas pueden satisfacer esta necesidad manteniendo una tabla centralizada de traducción de nombres a direcciones. Los PCs de la red pueden mantenerse actualizados si copian esta tabla periódicamente. Así es como comenzó la traducción de nombres a direcciones IP.

El Centro de información de red del Departamento de defensa (DoD NIC, *Department of Defense Network Information Center*) disponía de la versión maestra de la tabla de traducción de nombres a direcciones y otros sistemas realizaban una copia regularmente. Conforme fue pasando el tiempo, este método se fue haciendo pesado e ineficaz.

El **Sistema de nombres de dominio (DNS, Domain Name System)** se creó para proporcionar un método para seguir la pista a los nombres y direcciones en Internet. Las bases de datos DNS proporcionan servicios de conversión de nombre a dirección. Muchas organizaciones usan también DNS para registrar de forma interna los nombres de sus propios ordenadores.

Hoy en día el protocolo DNS se utiliza también en los sistemas operativos Windows, además de como mecanismo de resolución de nombres, para almacenar la base de datos del Directorio Activo. Sin embargo, antiguamente los sistemas Windows utilizaron otros métodos de resolución de nombres, principalmente NetBIOS.

1.1 NetBIOS

NetBIOS asocia un nombre lógico de 16 caracteres (incluido el carácter de fin de cadena), a la dirección física de cada tarjeta de red, recogiendo estas parejas de datos en una tabla de nombres. NetBIOS permite asignar 254 nombres a la vez. Los nombres NetBIOS pueden ser individuales o de grupo. Los primeros hacen referencia a una única máquina, mientras que en los segundos se transmiten mensajes a varios nodos a la vez, utilizando para ello servicios no orientados a conexión.

El espacio de nombres NetBIOS es plano, lo que significa que dichos nombres sólo se pueden utilizar una vez dentro de una red. Estos nombres se registran dinámicamente cuando se inician los equipos, los servicios o cuando los usuarios inician la sesión.

El archivo **Lmhosts** es un archivo estático que asiste en la resolución de nombres NetBIOS en los equipos que no pueden responder a las difusiones de consultas de nombres NetBIOS. Contiene asignaciones entre nombres NetBIOS y direcciones IP.

Cuando se inicia, NetBIOS registra el nombre usando una petición de registro de nombre (*name registration request*), que normalmente se realiza usando un mensaje de difusión. Comprueba que no existe ya, y devuelve un índice en caso de éxito para ser usado durante las comunicaciones. Si otro host está registrado con el mismo nombre NetBIOS, responde con un mensaje negativo de registro de nombre (*negative name registration response*). El host que está arrancando recibe un error de inicialización.

El gran problema que presentaba NetBIOS era que se basaba en mensajes de difusión, que no se transmiten en entornos enrutados. Es decir, las peticiones de registro no pasaban

a través de los routers. Para solucionar los problemas que ocasiona la resolución de nombres NetBIOS en entornos con rutas, Microsoft creó WINS.

1.2 WINS

El **Servicio de nombres Internet de Windows (WINS)** proporciona una base de datos distribuida en la que se registran y consultan asignaciones dinámicas de nombres NetBIOS para los equipos y grupos usados en la red. WINS asigna los nombres NetBIOS a direcciones IP.

WINS simplifica la administración del espacio de nombres NetBIOS en las redes TCP/IP. En un sistema WINS, todos los nombres están registrados en un servidor WINS. Los nombres están almacenados en una base de datos del servidor WINS que responde a las peticiones de resolución de nombres en direcciones IP basadas en las entradas de dicha base de datos.

La redundancia y el reparto de la carga se mantienen con varios servidores WINS en la red. Periódicamente, los servidores duplican las entradas de sus bases de datos entre ellos para mantener una vista coherente del espacio de nombres NetBIOS.

Todos los nombres tienen una entrada en la base de datos. Esa entrada es propiedad del servidor WINS con el que se registra y hay un duplicado en todos los demás servidores WINS.

WINS también permite el registro de nombres estáticos. Esto posibilita que el administrador registre nombres de servidores que ejecuten sistemas operativos que no puedan registrar fácilmente nombres de forma dinámica. WINS distingue entre entradas dinámicas y entradas estáticas. Los nombres estáticos se tratan de forma algo diferente que los dinámicos.

Entre las ventajas que proporciona WINS sobre NetBIOS tenemos:

- Base de datos dinámica (nombre a dirección) que permite el registro y la resolución de nombres de equipo.
- Administración centralizada de la base de datos nombre a dirección, con lo que se reduce la necesidad de administrar archivos Lmhosts.
- Reducción del tráfico de difusión NetBIOS en las subredes, ya que se permite a los clientes hacer consultas directamente a los servidores WINS.
- Resolución de nombres NetBIOS en sistemas encaminados, ya que los clientes pueden hacer consultas en los servidores WINS para encontrar sistemas remotos.

2. DNS

DNS es una base de datos distribuida. Los nombres y direcciones de Internet se almacenan en servidores de todo el mundo. Toda organización que posea un nombre de dominio es responsable del funcionamiento y mantenimiento de los servidores de nombres que traducen sus propios nombres a direcciones.

Puesto que la traducción de nombre a dirección es tan importante, la información se duplica en uno o varios servidores secundarios.

El esquema de DNS:

- Permite delegar la asignación de nombres y direcciones a un responsable de toda o parte de una red particular.
- Permite que los nombres reflejen la estructura lógica de una organización.
- Asigna direcciones que reflejan la topología lógica de la red de la organización.

A los servidores se les suelen dar nombres que sean fáciles de localizar. Por ejemplo:

- `www.iessanclemente.net`
- `ftp.microsoft.com`
- `www.google.es`

En los nombres DNS no hay diferencias entre las minúsculas y las mayúsculas. Por ejemplo, `www.iessanclemente.net` se podría escribir `WWW.IESSANCLEMENTE.NET` o `www.IESSanClemente.net`. Normalmente los usuarios escribirán los nombres en minúsculas, mientras que en algunas tablas aparecerán los nombres en mayúsculas.

2.1 Funciones de DNS

Además de la resolución de nombres, el DNS se utiliza también para otros propósitos relacionados, principalmente

- Resolución inversa de direcciones: es el mecanismo inverso al anterior. Consiste en, dada una dirección IP, obtener el nombre asociado a la misma.
- Resolución de servidores de correo: dado un nombre de dominio (por ejemplo `gmail.com`) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, `gmail-smtp-in.l.google.com`).
- Por tratarse de un sistema muy flexible, es utilizado también para muchas otras funciones, tales como la obtención de claves públicas de cifrado asimétrico y la validación de envío de e-mails (a través de mecanismos como SPF).

2.2 Terminología

Es necesario introducir algunos términos básicos para evitar confusiones y ambigüedades.

- **Host Name:** el nombre de un host es una sola “palabra” (formada por letras, números y guiones). Ejemplos de nombres de host son “www”, “blog” y “mestre”.

- **Fully Qualified Domain Name (FQDN):** es el “nombre completo” de un host. Está formado por el hostname, seguido de un punto y su correspondiente nombre de dominio. En algunos casos, sobre todo en los ficheros de configuración de DNS, los FQDN se escriben acabados en punto. Por ejemplo, “www.iessanclemente.net.”.
- **Domain Name:** el nombre de dominio es una sucesión de nombres concatenados por puntos. Las normas de nombres de Internet permiten que cada etiqueta pueda tener hasta 63 caracteres, y que un nombre pueda tener hasta 255 caracteres. Algunos ejemplos son “iessanclemente.net”, “google.com” y “es”.
- **Top Level Domains (TLD):** los dominios de nivel superior son aquellos que no pertenecen a otro dominio. Ejemplos de este tipo son “com”, “org” y “es”. Los dominios iessanclemente.net y google.com, se llaman dominios de segundo nivel (*second-level domains*).

2.3 Estructura Jerárquica de Nombres

Es muy fácil entender la estructura jerárquica de los nombres. Cada organización tiene un nombre superior descriptivo, como iessanclemente.net o microsoft.com. A partir de ahí, la organización tiene total libertad para elegir cualquier esquema de nombres que le resulte conveniente. Por ejemplo, el IES San Clemente puede crear subdominios para delegar la responsabilidad de los nombres a algunos departamentos, y a otros mantenerlos bajo su nombre genérico.

Por tanto, puede haber nombres que acaben en:

- informatica.iessanclemente.net
- esa.iessanclemente.net
- iessanclemente.net

Algunos departamentos pueden crear otra estructura de nombres en sus propios subdominios. Por ejemplo, podrían existir nombres como:

- matematicas.esa.iessanclemente.net
- lengua.esa.iessanclemente.net

Se pueden asignar nombres de cualquier forma que sea administrativamente conveniente, aunque las máquinas con un mismo sufijo no se encuentren en una misma LAN.

Si se usa una estructura jerárquica de nombres resulta más sencillo asegurarse de que todos los nombres son únicos, a la vez que se delega el trabajo de administración de los nombres al personal apropiado. Tenga en cuenta que:

- En cada subdominio de cada departamento (informática, esa), habrá un administrador encargado de asignar nombres distintos a las máquinas (www.informatica.iessanclemente.net, blog.informatica.iessanclemente.net).
- La responsabilidad de asignar nombres diferentes dentro de cada departamento (matemáticas, lengua, etc.) es del administrador de ese subdominio (esa.iessanclemente.net).
- Si el administrador de la red asigna a cada departamento un nombre de subdominio diferente (informatica, esa), todos los nombres de su red serán diferentes.

- Existen organismos de registro que se aseguran que las organizaciones tengan un nombre de dominio único (por ejemplo: iessanclemente.net, microsoft.com). Por tanto, cada ordenador del mundo puede tener un nombre único.

A menudo, resulta conveniente asignar algún alias o seudónimo, indicativo de su función, a un ordenador, además de su nombre real. Por ejemplo, si el host `exámenes.informatica.iessanclemente.net` ofrece servicios de transferencia de archivos, por conveniencia, se le puede asignar el siguiente alias:

```
ftp.informatica.iessanclemente.net
```

Si la carga en el host llega a ser muy alta, el servicio de transferencia de archivos, y su seudónimo se pueden transferir a un host diferente. De esta forma el usuario puede obtener el servicio usando el mismo nombre, aunque la máquina que da el servicio haya cambiado. El nombre real del host se denomina nombre canónico.

2.4 Relación entre zonas y servidores DNS

Los servidores DNS utilizan el puerto 53 del protocolo UDP.

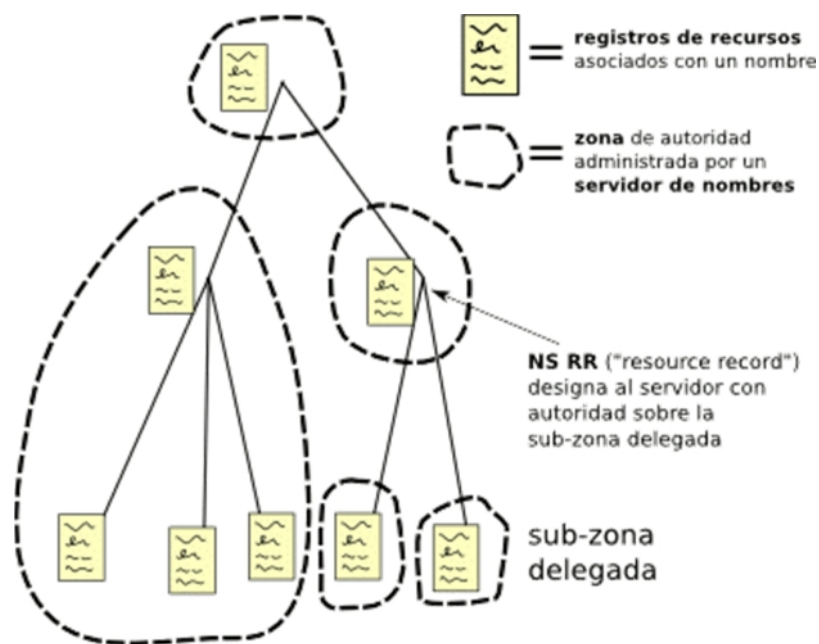
El sistema está estructurado en forma de árbol. Cada nodo del árbol está compuesto por un grupo de servidores que se encargan de resolver un dominio o un conjunto de dominios (zona de autoridad).

Un servidor puede delegar en otro (u otros) la autoridad sobre alguna(s) de sus sub-zonas (esto es, algún subdominio de una zona sobre la que él tiene autoridad). Estas sub-zonas se pueden almacenar, distribuir y replicar en otros servidores DNS.

La división en sub-zonas tiene las siguientes ventajas:

- Permite delegar la administración de parte del espacio de nombres DNS en otra ubicación o departamento de la organización.
- Permite dividir una zona de gran tamaño en zonas más pequeñas para distribuir las cargas de tráfico entre varios servidores, mejorar el rendimiento de la resolución de nombres DNS o crear un entorno DNS con mayor tolerancia a errores.

Por cada sub-zona que se crea, se necesitan registros de delegación que señalan a los servidores DNS autoritativos para la nueva sub-zona. Esto es necesario para transferir autoridad y proporcionar referencias correctas a los servidores y clientes DNS de los nuevos servidores que se están convirtiendo en autoritativos para la nueva zona.



Los servidores con autoridad sobre los TLD son los llamados “root servers” (o servidores raíz) del sistema. Estos son fijos, ya que rara vez cambian. Deben estar configurados correctamente en cualquier servidor DNS para que pueda propagar las consultas que recibe.

En función del papel que realicen para cada una de las zonas, un servidor DNS puede ser:

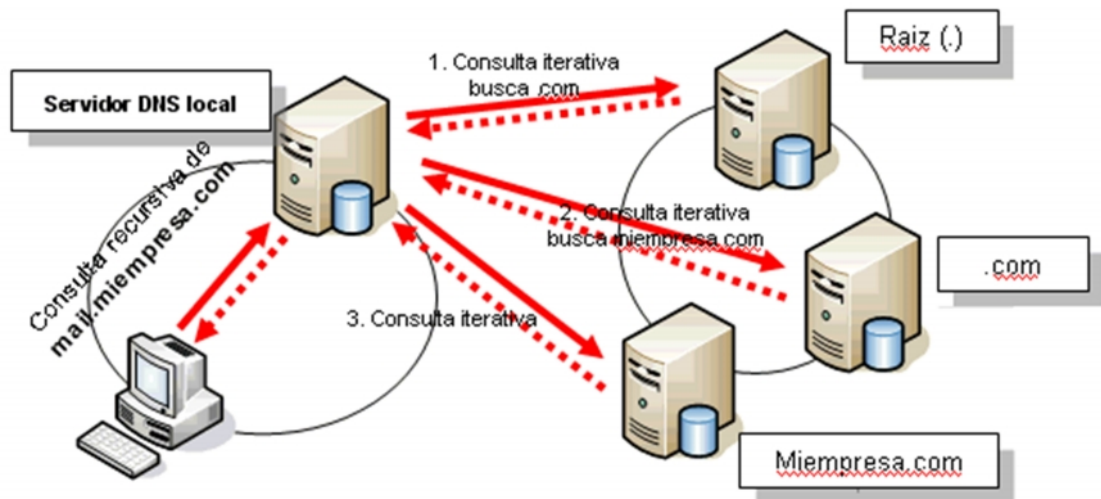
- **Servidor DNS primario:** es único y obligatorio para cada zona, siendo el único en el cual se podrá administrar, dando altas, bajas o modificando los registros correspondientes. Será, por así decirlo, el poseedor de la información original de la zona, ya que el resto de los servidores DNS, que tengan información de esa zona, tendrán una “copia de sólo lectura” de la misma.
- **Servidor DNS secundario o esclavo:** serán todos aquellos servidores DNS que tengan una copia completa de la zona determinada. Su copia se actualizará, automáticamente, a partir de la información de un DNS maestro. Este proceso se conoce con el nombre de transferencia de zona.

No es obligatoria su existencia y el número puede ser ilimitado. Se utilizan como medida de seguridad, frente a un fallo del DNS primario, y para la distribución de la carga del servicio DNS de la zona en cuestión. Un servidor puede ser secundario para una zona y primario para otra de forma simultánea.

- **Servidor DNS maestro:** todo aquel servidor que sirva de fuente para transferir una zona a otro servidor DNS, denominado esclavo. Un servidor DNS maestro, puede ser un servidor primario o un servidor secundario, esclavo, que actúe como maestro para un tercero.
- **Servidor DNS autoritativo:** todo aquel servidor DNS que se encuentre en condiciones de convertirse en DNS maestro de una zona y disponga del correspondiente registro NS definido en la zona en cuestión. Un servidor DNS, que tan sólo disponga de la información de una zona, aunque sea completa, a través de la caché de su servicio DNS, y no disponga de una copia activa en su propio servicio DNS, no será un servidor autoritativo de la zona en cuestión.

2.5 Proceso de resolución de nombres por un servidor DNS

Cuando un servidor DNS recibe una consulta de resolución de nombres, y no pertenece a su zona de autoridad, sigue el siguiente procedimiento:



- El servidor de nombres inicial o local consulta a uno de los servidores raíz (cuya dirección IP debe conocer previamente).
- Éste devuelve el nombre del servidor a quien se le ha delegado la sub-zona.
- El servidor inicial interroga al nuevo servidor.
- El proceso se repite nuevamente a partir del punto 2 si es que se trata de una sub-zona delegada.
- Al obtener el nombre del servidor con autoridad sobre la zona en cuestión, el servidor inicial lo interroga.
- El servidor resuelve el nombre correspondiente, si existe, y devuelve la dirección IP obtenida.
- Para disminuir el tráfico, el servidor inicial almacenará temporalmente las respuestas en caché en su disco duro. El tiempo máximo que permanece la información almacenada en la caché se configura en los servidores y se envía al solicitante junto con el resultado de la consulta.

En este proceso se dice que el cliente realiza una **consulta recursiva** porque es la única que hace directamente, aunque a su vez el destinatario de la consulta tenga que hacer otras para obtener la resolución.

Por su parte, el servidor de nombres inicial realiza una **consulta iterativa**, esto es, emplea distintos servidores DNS para realizar las consultas directas que sean necesarias en la resolución del nombre.

2.6 Clientes DNS

Un programa cliente capaz de consultar información en el Sistema de nombres de dominio es parte estándar de los productos TCP/IP y se denomina un **resolutor**. Normalmente, un resolutor trabaja discretamente en segundo plano y los usuarios ni siquiera lo notan. Por ejemplo, cuando un usuario hace un ping a `www.iessanclemente.net`, el programa ping llama al resolutor local que busca su dirección IP:

```
ping iessanclemente.net
Haciendo ping a iessanclemente.net [82.98.132.209] con 32 bytes de datos:
Respuesta desde 82.98.132.209: bytes=32 tiempo=53ms TTL=52
```

Pero, ¿de dónde obtiene la información el resolutor? Dependiendo del sistema operativo de que estemos hablando, esta pregunta tiene distintas respuestas. En sistemas Linux existen dos archivos llamados `resolv.conf` y `nsswitch.conf` que contienen datos sobre cómo obtendrá información.

- **/etc/nsswitch.conf** contiene el orden en que el sistema consultará a distintos orígenes de datos, incluyendo la resolución de nombres. El fichero contendrá una línea como la siguiente:

```
hosts: files dns
```

El significado de estos parámetros es que cualquier tipo de resolución de nombres primero debe buscar en el archivo **/etc/hosts** y posteriormente consultar a los servidores DNS configurados en el equipo.

El fichero `/etc/hosts` contiene una resolución estática de nombres a direcciones IP. En algunas ocasiones se opta por este tipo de resolución debido a su rapidez ya que la información reside en el mismo equipo que está solicitando la resolución. Sin embargo, una de las desventajas que presenta este archivo es que debe ser modificado manualmente.

En la actualidad, algunos sistemas Linux (por ejemplo Ubuntu Desktop) incluyen un sistema (AVAHI) que utiliza MDNS (DNS Multicast) como mecanismo de descubrimiento de servicios en una red local. Con tal fin acapara el TLD **.local**, con lo que no funcionarán las búsquedas de nombres DNS bajo ese TLD.

Una forma de solucionarlo es editar el fichero `nsswitch.conf` para eliminar la búsqueda DNS Multicast, o retrasarla en el orden de la línea `hosts`.

Anteriormente los sistemas Linux usaban con este fin el fichero **/etc/host.conf**, que normalmente contenía una línea parecida a:

```
order hosts, bind
```

- **/etc/resolv.conf** coordina información sobre cómo serán utilizados los servidores BIND. Este archivo define varios parámetros. La parte más importante son los parámetros **nameserver**, que indican cuáles son las direcciones IP de los servidores DNS que deben ser utilizados, por ejemplo.

```
nameserver 172.16.1.254
nameserver 172.16.1.252
```

Es importante tener en cuenta que, tanto en sistemas Windows como Linux, la respuesta obtenida del primer servidor de nombres es la válida, sea positiva (se ha conseguido resolver el nombre por una dirección IP) o negativa (no se ha encontrado el nombre bus-

cado). Los restantes servidores de nombres configurados en el resolutor, si existen, solo se consultarán en caso de que no se haya podido contactar con ninguno de los que les preceden en la lista.

En sistemas Windows la configuración es muy similar a la de Unix, sin embargo, debido a su sencillez no es tan flexible. En Unix es posible especificar el orden en que serán utilizados ciertos servicios para la resolución de nombres (archivo `/etc/nsswitch.conf`), pero en Windows la resolución se lleva a cabo automáticamente de la siguiente manera:

- Verificar el archivo `hosts`. El archivo `hosts` en Windows es idéntico al utilizado por Unix. Contiene la dirección IP y el nombre completo de cada uno de los equipos a los que se refiere.
- Intentar una resolución con los servidores DNS especificados. Al igual que se hace en Linux utilizando el archivo `/etc/resolv.conf` en Unix, Windows también es capaz de especificar cuáles y cuantos servidores DNS serán utilizados. La metodología en Windows es gráfica y se encuentra accesible a través del Panel de Control.

Una vez que un resolutor resuelve un nombre, almacena temporalmente esa información en memoria caché. En entornos Windows, podemos ver el contenido de esa memoria haciendo

```
ipconfig /displaydns
```

Y borrarse ejecutando el comando

```
ipconfig /flushdns
```

En Linux para hacer eso mismo se debe reiniciar el demonio de la caché del servicio de nombres, **nsd** (*name service cache daemon*).

2.7 Servidores DNS

El software más utilizado en los servidores de nombres de Internet es **BIND** (*Berkeley Internet Name Domain*), creado originalmente en la Universidad de California. Históricamente es el software que usan los servidores raíz, sin embargo para prevenir el problema que puede suponer un fallo de seguridad en BIND, hoy en día algunos de los servidores raíz utilizan otro software: NSD (www.nlnetlabs.nl/projects/nsd).

Existen versiones de BIND para sistemas Unix/Linux y para sistemas Windows. Además, las versiones servidor de Windows incluyen su propio software servidor DNS.

2.8 Ficheros de zona

La forma en que se almacenan los datos del DNS depende del software servidor utilizado. En la gran mayoría se guardan como una serie de entradas de texto.

Existen tres tipos de entradas:

- **Comentarios.** Comienzan por un punto y coma, y se pueden colocar a continuación de otra entrada o en una línea nueva.

- **Directivas.** Comienzan por un signo \$, y controlan la forma en que se procesa el fichero de zona.
- **Registros de recursos**, o RR (*Resource Record*). Definen las características o las entidades de la zona. Hay varios tipos de registros de recursos, cada uno identificado por un carácter o un acrónimo corto. Si se extienden más de una línea, se deben usar paréntesis.

Las directivas que nos podemos encontrar en una zona son:

- **\$TTL.** Define el valor por defecto del campo TTL para la zona. Esta directiva es obligatoria.
- **\$ORIGIN.** Define el dominio de la zona. Su uso es opcional.

Un registro de recursos contiene líneas de tipo:

```
[nombre] [TTL] [clase] Tipo Datos
```

Los campos de un registro de recursos se separan por espacios o tabulaciones.

Si se omiten los valores de nombre o clase, por defecto son los últimos que se hayan indicado con anterioridad. Actualmente, la única clase utilizada es “IN” para Internet, por lo que este campo suele aparecer sólo una vez, en el primer registro.

El tiempo de vida (**TTL**, *Time-To-Live*) indica cuánto tiempo debe guardarse cada registro en la caché después de almacenarse. El orden de los campos clase y TTL puede intercambiarse. TTL es numérico y, por lo tanto, no se puede confundir con la clase.

Ejemplo de archivo:

```
; fichero de la zona sanclemente.net
$TTL 12h ; en BIND los valores de tiempo se pueden poner de forma abreviada
$ORIGIN sanclemente.net.
sanclemente.net.      IN      SOA      ns.sanclemente.net.
                        postmaster.sanclemente.net. (
                        201209172016 ;      número de serie
                        86400        ;      refrescar tras 24 horas
                        3600         ;      reintentar tras 1 hora
                        2592000      ;      expira tras 30 días
                        7200         ;      nxwas de 2 horas
                        )

sanclemente.net.      IN      ns       ns.sanclemente.net.

localhost              IN      A        127.0.0.1
ns                     IN      A        172.66.1.1
ns2                    IN      A        172.66.1.100

mail-relay             IN      A        172.66.1.2
                      IN      TXT      www, ftp on mail-relay
                      IN      TXT      gopher on mail-relay
                      IN      HINFO     SUN UNIX
```

```

www                IN      CNAME  mail-relay
ftp                IN      CNAME  mail-relay
gopher             IN      CNAME  mail-relay

sanclemente.net.  IN      MX      1      mail-relay
*                  IN      MX      1      mail-relay
ns                 IN      MX      1      mail-relay
; fin del fichero de zona sanclemente.net

```

En un fichero de zona existen principalmente los siguientes tipos de registros de recursos:

- **SOA:** identifica el dominio o la zona y fija una serie de parámetros. Es el primer registro del archivo es muy importante. Se trata del registro de Inicio de autoridad (SOA, *Start of Authority*). El paréntesis en el registro SOA le permite extenderse varias líneas. En el registro se incluyen varios valores de temporización, medidos en segundos. En el ejemplo anterior, el registro SOA indica que:
 - El servidor ns.sanclemente.net es primario para el dominio sanclemente.net, el que posee la información original de la misma (a través de él se administra, dando bajas, altas, etc.).
 - Se deben comunicar los problemas a postmaster@sanclemente.net (cambiando el primer punto por @).
 - Los servidores secundarios copiarán este archivo completo y obtendrán información importante de los cuatro siguientes elementos del registro SOA. Cada servidor secundario debería:
 - Conectarse al primario cada 24 horas.
 - Comprobar si su número de serie actual es menor que el del primario.

Para ello solicita una actualización de una zona al correspondiente maestro, que le envía una copia del registro SOA.

Si comprueba si el valor del campo número de serie es mayor que el que tiene la copia de la zona que él posee, se ha actualizado el primario y el secundario necesita realizar una transferencia de zona, es decir, copiar en su sistema la base de datos completa para esa zona.

Cada vez que se haga un cambio en un fichero de zona, se deberá incrementar su número de serie, para posibilitar la transferencia de zona a los esclavos.

- Si el secundario no logra conectarse a la hora prevista debería intentarlo de nuevo 1 hora más tarde.
 - Si el secundario no es capaz de contactar con el primario en un período de 30 días, debe dar por caducados todos los datos y dejar de responder a consultas.
 - Si el registro que se solicitaba no existe, el error obtenido puede guardarse en caché durante 2 horas. Este parámetro puede variar entre 0 y un máximo de 3 horas.
- **NS:** hace corresponder el nombre de dominio con el nombre de un servidor de nombres del dominio. A diferencia del SOA el registro NS puede no ser único, ya que debe existir uno por cada DNS secundario autoritativo de la zona, más el correspondiente al DNS primario, que sí es obligatorio en cada zona.

Si hay subzonas se necesitan entradas para los servidores de nombres de las subzonas “hijas” de forma que el servidor de más alto nivel pueda facilitar apuntadores a los ser-

vidores de bajo nivel. También se necesitan registros de direcciones para poder acceder a esos servidores hijo.

En el fichero de configuración de una zona, un nombre que no termina en punto se completa añadiéndole el Nombre de dominio de esa zona (sanclemente.net.). Por ejemplo, en ese archivo, ns corresponde a ns.sanclemente.net.

- **A:** hace corresponder el nombre de un sistema con su dirección (Address). Esos registros de direcciones se denominan registros de asociación. Si un sistema, por ejemplo, un encaminador, tiene varias direcciones, habrá un registro diferente para cada una de ellas.
- **AAAA:** es el equivalente de A, pero realizando la asociación con direcciones IPv6, en lugar de IPv4.
- **CNAME:** alias. En ocasiones se instalan varios servicios en una misma máquina, y para facilitar el acceso a los usuarios, mediante nombres que le sean sencillos y próximos al servicio que demandan, resulta interesante que esa máquina responda a distintos nombres DNS.

Por ejemplo, imagine que en un mismo servidor instala un servidor web y un servidor FTP, quizá lo más razonable sea indicarle al usuario que la empresa dispone de un sitio web en la dirección `www.iessanclemente.net` y de un servidor FTP en la `ftp.iessanclemente.net`, sin importarle si responden en el mismo servidor o distintos.

La función del registro CNAME es precisamente esa. Hace corresponder un alias con el nombre canónico de un host.

Aunque en muchos casos también sería posible utilizar un nuevo registro de tipo A para definir el host `ftp.iessanclemente.net`, sin necesidad de usar el alias (CNAME), se prefiere utilizar el alias para evitar multiplicidades de direcciones IP en el registro DNS, lo que complica la administración del servicio DNS, y es una posible fuente de errores por olvidar la actualización de la IP en alguno de los registros DNS del servidor con múltiples nombres registrados.

El único caso en que no sería posible sustituir un registro CNAME por un registro A, es cuando el nombre del host real no pertenece al mismo dominio.

```
ftp      IN      CNAME  ftp.iessanclemente.org.
```

- **MX:** intercambiador de correo (*Mail Exchanger*). Identifica a los sistemas que se encargan del correo de la organización. El comodín (*) permite reenviar correo dirigido a hosts determinados que no aparecen listados en el directorio del DNS. Los números que aparecen después de MX se llaman números de prioridad, y se utilizan para proveer servidores de respaldo que entren en funcionamiento en caso de fallo del servidor de correo principal.
- **TXT:** proporciona una forma de añadir comentarios de texto a la base de datos. Por ejemplo, un registro TXT podría hacer corresponder `sanclemente.net` con el nombre, dirección y número de teléfono de la compañía.
- **PTR:** hace corresponder una dirección IP con el nombre de un sistema. Usado en archivos para resolución inversa dirección - nombre.
- **SPF:** se utiliza para identificar a los remitentes autorizados de correo, como vemos en la siguiente sección.

En los ficheros de definición de zonas es habitual encontrar el carácter @ sustituyendo el nombre de la zona. Este carácter hace que se tome como nombre de zona el mismo que se utilizó para referenciar la zona en la configuración del servidor DNS.

2.9 Resolución inversa

La resolución inversa se utiliza para asociar direcciones IP a nombres, de forma inversa a la resolución habitual de DNS.

Cuando se utiliza el fichero hosts, la resolución se realiza mediante una búsqueda simple en el fichero. Si utilizamos DNS, las direcciones inversas se ubican bajo un dominio especial: **in-addr.arpa**, que contiene las direcciones IP de todos los sistemas en una notación de puntos invertida. Por ejemplo, a la dirección 1.2.3.4 le corresponde el nombre 4.3.2.1.in-addr.arpa. El registro de recurso (RR) que define esto se llama registro PTR.

Por ejemplo, para realizar resolución inversa en la red 172.66.1.0/24, tendríamos que crear el siguiente fichero:

```
; fichero de la zona inversa 1.66.172.in-addr.arpa
@ IN SOA ns.sanclemente.net. postmaster.sanclemente.net. (
                                1999090200 360000 3600 3600000 3600
                                )
1      IN      PTR      ns.sanclemente.net.
2      IN      PTR      mail-relay.sanclemente.net.
100    IN      PTR      ns2.sanclemente.net.
```

2.10 Utilizar DNS para asegurar los remitentes de correo

Los registros de tipo MX de un servidor DNS sirven para indicar qué máquina es la que ejecuta un servidor de correo para un dominio determinado. El procedimiento general de envío de correo es el siguiente:

1. Un usuario a, con dirección de correo a@hotmail.com, quiere enviar un correo a otro usuario b, con dirección de correo electrónico b@gmail.com.
2. El usuario a escribe el correo y se lo envía a su servidor de correo, que se aloja en la máquina A. Para realizar esta operación se utiliza normalmente un protocolo que requiere autenticación del usuario.
3. El servidor de correo en A busca el servidor de correo de b@gmail.com. Para eso realiza una consulta DNS de solicitud de registros tipo MX para el dominio gmail.com y obtiene su dirección IP.
4. El servidor de correo de A se pone en contacto con el servidor de correo de gmail.com y le envía el mensaje.

El principal problema de seguridad de este método es el punto 4. Si no se realiza ningún tipo de autenticación en el envío de correo entre servidores, cualquiera puede decir que es el servidor de correo de Hotmail y enviar correo a GMail en su nombre.

La solución es un estándar llamado SPF (*Sender Policy Framework*). La idea es que cada dominio publique en la definición DNS de su zona la lista de máquinas que están au-

torizadas a enviar correo en su nombre.

Es decir, si Hotmail añade un registro SPF, cuando el servidor de correo de GMail recibe el correo verificará si el remitente está o no autorizado a enviarlo. Obviamente, para que esto sea posible, además de crear el registros correspondiente, el servidor de correo receptor (en nuestro caso el de GMail) deberá soportar SPF y realizar la verificación oportuna.

Tipos de registro SPF

Los registros SPF pueden almacenarse en un registro de tipo TXT, o en su propio tipo de registro SPF (creado con este fin). Preferiblemente deberán figurar ambos tipos de registro con contenido idéntico.

Su contenido comenzará definiendo la versión de SPF implementada, y a continuación una serie de reglas que se evaluarán en el orden en que figuren en el registro. Cada regla puede indicar a que máquinas se les permite (signo + o sin signo) o no se les permite (signo -) enviar correo procedente del dominio.

Cuando se produce una coincidencia, se aplica lo que indique la regla. Si se procesan todas las reglas sin encontrar coincidencia, por defecto se permite el envío de correo.

Por ejemplo, un registro de tipo SPF podría ser:

```
sanclemente.local.  SPF      v=spf1 mx a:correo.sanclemente.local -all
sanclemente.local.  TXT      v=spf1 mx a:correo.sanclemente.local -all
```

Es decir:

- Primero se comprueba si la máquina que envía el correo se corresponde con un registro de tipo MX, en cuyo caso se permite el envío.
- Si no coincide la regla anterior, se comprueba si se corresponde con el registro tipo A de correo.sanclemente.local, en cuyo caso también se permite el envío.
- Por último, el resto de máquinas no están autorizadas.

2.11 DNSSEC

La información que se solicita a los servidores DNS es pública. Cualquiera puede acceder a ella, y por lo tanto no es necesario cifrar su transmisión. Sin embargo, es posible que alguien suplante a un servidor DNS y ofrezca información falsa en respuesta a las consultas recibidas. Y ese es un problema de seguridad importante.

Si queremos consultar la página web de un buscador como google, y nuestro navegador en su lugar nos dirige a un sitio con publicidad, es un problema menor. Pero si queremos entrar en nuestro banco on-line, el falso servidor DNS puede redirigirnos a otro sitio con su misma apariencia que obtenga nuestras claves secretas. Y en este caso el problema puede ser bastante más grave.

DNSSEC, **Extensiones de Seguridad para DNS** (*Domain Name System Security Extensions*), es un mecanismo que permite firmar digitalmente la información que recibimos de un servidor DNS, de manera que se pueda asegurar que el que nos la ha enviado es quién dice ser, y que ésta ha llegado hasta nosotros completa y sin modificaciones.

Los servidores que implementan DNSSEC incluyen, junto a la información propia de cada una de las zonas que gestionan, registros de recursos propios de la extensión. Estos

tipos de registros son:

- RRSIG
- DNSKEY
- DS
- NSEC
- NSEC3
- NSEC3PARAM

Cuando se usa DNSSEC, cada respuesta que envía el servidor correspondiente a una solicitud va acompañada de un registro adicional de tipo RRSIG, que se corresponde con la firma correspondiente a esa respuesta concreta.